DATE(S) ISSUED:

12/10/2013

SUBJECT:

Vulnerability in Windows Could Allow Remote Code Execution (MS13-098)

OVERVIEW:

A vulnerability has been discovered in Microsoft Windows that could allow a remote attacker to take complete control of a vulnerable system. This vulnerability can be exploited when a user opens a specially crafted executable file. Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- · Windows XP

- · Windows Vista

- · Windows 7

- · Windows 8

- · Windows RT

- · Windows Server 2003

- · Windows Server 2008

- · Windows Server 2012

RISK:

Government:

- · Large and medium government entities: **High**

- · Small government entities: **High**

Businesses:

- · Large and medium business entities: **High**

·   Small business entities: **High**

Home users: High

DESCRIPTION:

A vulnerability has been discovered in Microsoft Windows that could allow a remote attacker to take complete control of a vulnerable system. The vulnerability is caused by the way that the WinVerifyTrust function handles Windows Authenticode signature verification for portable executable (PE) files. PE is the common executable file format for Windows. An attacker may modify unverified portions of an existing signed executable file to include malicious code without invalidating the signature. This vulnerability can be exploited if a user opens a specially crafted PE file.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- ·   Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- ·   Remind users not to download, accept, or execute media files from un-trusted or unknown sources.
- ·   Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- ·   Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:

http://technet.microsoft.com/en-us/security/bulletin/ms13-098

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3900